CLAIMS

What is claimed is:

1 1. An apparatus for performing multistage processing with feedback, comprising:
2 a first plurality of processing stages connected in series and having a feedback
3 channel connecting a last stage of the first plurality to one of the processing
4 stages among the first plurality of processing stages, wherein each processing
5 stage of the first plurality is configured to process one block of data from a
6 data stream during one processing cycle; and
7 a parallel input queue comprising a second plurality of input queues connected in
8 parallel to the first stage, and configured to direct a data block to the first stage
9 alternately from each of a third plurality of data streams.

1 2. An apparatus as recited in Claim 1, wherein the number of input queues in the second
2 plurality is no greater than a number of processing stages in the first plurality.

1 3. An apparatus as recited in Claim 1, wherein
2 a block on the feedback channel based on an input block on a particular data stream is
3 combined with a later block of the particular data stream that is a delay
4 number of blocks after the input block; and
5 a number of input queues in the second plurality is based on the delay number and a
6 number of processing stages in the first plurality.

1 4. An apparatus as recited in Claim 1, further comprising a parallel context array
2 comprising a second plurality of context registers connected in parallel to the first stage, for
3 directing context information from a context register to the first stage during a processing
4 cycle with an associated data stream on a corresponding input queue.

1   5.   An apparatus as recited in Claim 4, wherein the first plurality of processing stages

2   implement an encryption process and the context information associated with the data stream

3   comprises an encryption key for the data stream:

1   6.   An apparatus as recited in Claim 3, wherein the feedback channel comprises a set of

2   one or more feedback hold registers for synchronizing the block on the feedback channel to

3   be directed to the first stage during a processing cycle when the later block is directed to the

4   first stage.

1   7.   An apparatus as recited in Claim 1, further comprising a parallel output queue

2   comprising a second plurality of output queues connected in parallel to the last stage, for

3   directing a block from the last stage alternately to each of a third plurality of output streams,

4   each output stream corresponding to a respective data stream of the third plurality of data

5   streams.

1   8.   A method of performing multistage processing with feedback, the method comprising

2   the step of directing alternately to a first processing stage of a first plurality of processing

3   stages connected in series, a second plurality of data streams, wherein:

4   one data block from one data stream can be processed at one processing stage during

5   one processing cycle;

6   each interior input block of each data stream is not directed to the first processing

7   stage before an output block based on a previous input data block from the

8   data stream is output from the first plurality of processing stages;

9   the previous input data block precedes the interior input block in the data stream by a

10   delay number of blocks less than a number of processing stages in the first

11   plurality; and

12   the interior block follows the delay number of blocks counting from a beginning of

13   the data stream.

-27-

1   9.   A method as recited in Claim 8, wherein a number of data streams in the second

2   plurality is equal to the number of processing stages in the first plurality.

1   10.   A method as recited in Claim 8, wherein a number of data streams in the second

2   plurality is based on the number of processing stages and the delay number.

1   11.   A method as recited in Claim 8, further comprising the step of directing to the first

2   processing stage, with each data stream, context information associated with the data stream.

1   12.   A method as recited in Claim 11, wherein the first plurality of processing stages

2   implement an encryption process and the context information is an encryption key:

1   13.   A computer-readable medium carrying one or more sequences of instructions for

2   performing multistage processing with feedback, which instructions, when executed by one

3   or more processors, cause the one or more processors to carry out the step of

4   directing alternately to a first processing stage of a first plurality of processing stages

5   connected in series, a second plurality of data streams;

6   wherein

7   one data block from one data stream can be processed at one processing stage

8   during one processing cycle,

9   each interior input block of each data stream is not directed to the first

10   processing stage before an output block based on a previous input data

11   block from the data stream is output from the first plurality of

12   processing stages

13   the previous input data block precedes the interior input block in the data

14   stream by a delay number of blocks less than a number of processing

15   stages in the first plurality, and

16   the interior block follows the delay number of blocks counting from a

17   beginning of the data stream.

-28-

1   14.   An apparatus for performing multistage processing with feedback, comprising:

2   means for processing a data block sequentially through a first plurality of processing

3   stages connected in series during a corresponding number of clock cycles;

4   means for feeding an output block from a last stage of the first plurality back to a first

5   stage of the first plurality; and

6   means for directing a data block to the first stage alternately from each of a third

7   plurality of data streams on a parallel input queue comprising a second

8   plurality of input queues connected in parallel to the first stage.

1   15.   A method of designing a multistage processor with feedback to implement a

2 procedure, the method comprising the steps of:

3   identifying a number of stages and a feedback delay number of blocks for the

4   procedure;

5   providing for connecting the number of stages in series;

6   providing for a feedback channel connecting a last stage to a first stage;

7   determining whether the delay number is less than the number of stages;

8   if it is determined the delay number is less, then

9   determining a number of input queues based on the number of stages and the

10   delay number, and

11   provide for a parallel input queue comprising the number of parallel input

12   queues connected in parallel to the first stage.

1   16.   A method of fabricating a multistage processor with feedback to implement a

2 procedure, the method comprising the steps of:

3   identifying a number of stages and a feedback delay number of blocks for the

4   procedure;

5   connecting the stages in series;

6   forming a feedback channel connecting a last stage to a first stage;

7   determining whether the delay number is less than the number of stages;

8   if it is determined the delay number is less, then

50325-0506 (Seq. No. 2853)

9		determining a number of input queues based on the number of stages and the
10		delay number, and
11		forming a parallel input queue comprising the number of parallel input queues
12		connected in parallel to the first stage.

1	17.	An apparatus for encrypting or decrypting network messages on a data network,
2		comprising:
3		a network interface that is coupled to the data network for receiving a plurality of data
4		streams therefrom;
5		multiple processors connected in series and configured to process a data block from
6		an input stream during one processing cycle in one processor; and to feed an
7		output block from a last processor back to a first processor; and
8		a parallel input queue comprising a plurality of input queues connected in parallel to
9		the first processor for directing a data block to the first processor alternately
10		from each of the plurality of data streams.

1	18.	An apparatus as recited in Claim 17, further comprising:
2		a context channel connecting the multiple processors in series; and
3		a context buffer comprising a plurality of context registers connected in parallel to the
4		first processor for directing context information alternately from each of the
5		context registers to the first stage.

1	19.	An apparatus as recited in Claim 18, wherein the context information comprises a
2		symmetric block cipher encryption key associated with the data block.

1	20.	An apparatus as recited in Claim 18, wherein the context information comprises one
2		or more initial vector values associated with the data block for use as input to a
3		symmetric block cipher that encrypts the data block.

50325-0506 (Seq. No. 2853)

1   21.   A computer-readable medium carrying one or more sequences of instructions for
2   performing multistage processing with feedback, which instructions, when executed
3   by one or more processors, cause the one or more processors to carry out the steps of:
4   creating and storing a first plurality of processing stages that are connected in series
5   and having a feedback channel connecting a last stage of the first plurality to
6   one of the processing stages among the first plurality of processing stages;
7   creating and storing a parallel input queue comprising a second plurality of input
8   queues connected in parallel to the first stage;
9   processing one block of data from a data stream during one processing cycle using
10   each processing stage of the first plurality;
11   directing a data block to the first stage alternately from each of a third plurality of data
12   streams.

1   22.   A computer-readable medium as recited in Claim 21, wherein the instructions for
2 creating and storing a parallel input queue comprise instructions for creating and storing a
3 parallel input queue comprising a second plurality of input queues connected in parallel to the
4 first processing stage, wherein the number of input queues in the second plurality is no
5 greater than a number of processing stages in the first plurality.

1   23.   A computer-readable medium as recited in Claim 21, further comprising instructions
2 for carrying out the steps of:
3   combining a block on the feedback channel based on an input block on a particular
4   data stream with a later block of the particular data stream that is a delay
5   number of blocks after the input block;
6   creating and storing a number of input queues in the second plurality that is based on
7   the delay number and a number of processing stages in the first plurality.

-31-

1   24.   A computer-readable medium as recited in Claim 21, further comprising instructions

2   for carrying out the steps of:

3   creating and storing a parallel context array comprising a second plurality of context

4   registers connected in parallel to the first stage;

5   directing context information from a context register to the first stage during a

6   processing cycle with an associated data stream on a corresponding input

7   queue.

1   25.   A computer-readable medium as recited in Claim 24, further comprising instructions

2   for carrying out the steps of:

3   implementing an encryption process in the first plurality of processing stages;

4   creating and storing an encryption key for the data stream as the context information

5   associated with the data stream.

1   26.   A computer-readable medium as recited in Claim 23, further comprising instructions

2   for carrying out the steps of creating and storing, as part of the feedback channel, a set of one

3   or more feedback hold registers for synchronizing the block on the feedback channel to be

4   directed to the first stage during a processing cycle when the later block is directed to the first

5   stage.

1   27.   A computer-readable medium as recited in Claim 21, further comprising instructions

2   for carrying out the steps of: creating and storing a parallel output queue comprising a second

3   plurality of output queues connected in parallel to the last stage; and directing a block from

4   the last stage alternately to each of a third plurality of output streams, each output stream

5   corresponding to a respective data stream of the third plurality of data streams.

50325-0506 (Seq. No. 2853)